USAWC STRATEGY RESEARCH PROJECT

SPACE TECHNOLOGY AND NETWORK CENTRIC WARFARE: A STRATEGIC PARADOX

by

Lieutenant Colonel Karl Ginter
United States Army

Dr. Clayton K. S. Chun
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 MAR 2007	**Strategy Research Paper**	**00-00-2006 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Space Technology and Network Centric Warfare A Strategic Paradox	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Karl Ginter	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College,Carlisle Barracks,Carlisle,PA,17013-5050	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**22**	

ABSTRACT

AUTHOR: Lieutenant Colonel Karl Ginter

TITLE: Space Technology and Network Centric Warfare: A Strategic Paradox

FORMAT: Strategy Research Project

DATE: 22 February 2007 WORD COUNT: 6198 PAGES: 22

KEY TERMS: Space, Satellite, Global Information Grid, Information Technology

CLASSIFICATION: Unclassified

The Department of Defense (DoD) force transformation is in large measure predicated on harnessing and exploiting the benefits of shared information on the battlefield to develop a common operating picture. The DoD's aggressive pursuit of information technologies to enable network centric warfare (NCW) will generate a significant warfighting advantage as well as potential pitfalls. The Global Information Grid (GIG) is the telecommunications infrastructure—the network backbone—by which the United States facilitates NCW and executes its dominant forms of strategic power, both economically and militarily. A significant portion of the GIG relies upon space-based assets and technologies that expose the United States to vulnerabilities—the very same space-based technologies that enable NCW. This paper addresses threats to the GIG, vulnerabilities of our space-based assets, and examines concerns about the implicit reliance upon space-based technologies to execute NCW. It evaluates the strengths and weaknesses of employing space technology in a network centric environment, considers future threats posed by adversaries using asymmetric warfare, and examines the impacts on warfighting capabilities and national security. Finally, this paper identifies and recommends measures that mitigate risk to the United States' principal enabler of NCW—space-based technology.

SPACE TECHNOLOGY AND NETWORK CENTRIC WARFARE: A STRATEGIC PARADOX

The network centric warfare (NCW) concept of developing and leveraging information superiority by synchronizing sensors and shooters provides commanders with greater battlespace awareness and greatly enhances the warfighting capabilities for the U.S. military. A remarkable paradox of NCW and its heavy reliance upon space-based assets and technology is that the very capabilities that enable information sharing on the battlefield makes them increasingly vulnerable to a host of emerging threats. The growing network and communications interconnectivity of the GIG, both terrestrial and space, poses enormous risks to our command and control capabilities, information systems, and essential computer operations that enable battle command. These vulnerabilities also impact political and diplomatic means to achieve national security goals.

Some of the key enabling technologies of NCW are the Global Positioning System (GPS), communications satellites (both military and commercial), and our voice and data networks—all placing critical information at the fingertips of the warfighters.[1] These systems have inherent vulnerabilities that can, have, and will be exploited by our adversaries. Adversaries such as terrorist cells, organized crime, transnational groups, and nation-states who can not compete militarily or financially with the United States' robust information technology capabilities are identifying network vulnerabilities and developing relatively inexpensive attack capabilities to exploit these risks.[2] Moreover, the proliferation of vast, networked, computer-based capabilities that employ space assets as primary enablers can expect to encounter increased incidence of natural phenomena, human error, and technical failures.

This paper examines NCW's reliance upon space-based assets, and argues that the unchecked rapid development and integration of information technologies, specifically space-based technologies, into the military battle command infrastructure exposes the United States to vulnerabilities that bear close examination in order to mitigate potential threats that could impact U.S. military warfighting capability and national security.

Background

NCW has been the centerpiece of thought and dialogue on the future of warfighting since the mid-1990s. The theory of NCW was first espoused by VADM Arthur Cebrowski and John J. Garstka in a seminal 1998 article, "Network-Centric Warfare: Its Origin and Future."[3] Recognizing the advantages afforded the military by technology advancements of the information age, the authors explained the potential of NCW as follows:

> NCW is about human and organizational behavior. NCW is based on adopting a new way of thinking—network-centric thinking—and applying it to military operations. NCW focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces (consisting of entities) to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent.[4]

The essential tenets of NCW are: improved information sharing through a robustly networked force, enhanced quality of shared information and collaboration, and self-synchronization through shared situational awareness.

Most observers view technology as a dynamic force of transformation, and the United States accords a high priority and a great deal of resources to technology, specifically information technology (IT). The IT wave created the conditions that spawned NCW concepts and convinced DoD to pursue an aggressive policy to develop NCW capabilities designed to transform the U.S. military, with the goal of securing an IT-enabled warfighting advantage. The common denominator at some level for many of the IT systems that enable NCW, directly or indirectly, is space-based technology and the ability to gather and disseminate information across the extended battlespace. The business community has also embraced knowledge management, IT, and enterprise networking in order to enable innovation and gain a competitive advantage in the marketplace. The magnitude of corporate and military investments can not be understated. United States businesses alone have spent nearly $1 trillion a year since 2003 on IT equipment and services.[5] General Richard B. Myers, former Chairman of the Joint Chiefs of Staff, defined the magnitude of the DoD's commitment to transformation, stating, "For fiscal year 2003, the Department of Defense has requested nearly $128 billion for current and future weapons systems and capabilities."[6] Clearly, NCW plays a dominant role in reshaping the military and in the conduct of warfare in the information age.

The U.S. Congress has also levied NCW requirements on the DoD. In Section 934 of the Fiscal Year 2001 Defense Authorization Act (Public Law 106-398), Congress required the Secretary of Defense, in consultation with the Chairman of the Joint Chiefs of Staff (CJCS), "to develop a report on the development and implementation of network-centric warfare concepts within the Department of Defense." The act specifically stipulated that the Secretary and CJCS address the following areas: (1) a clear definition of NCW; (2) an accounting of NCW-related activities; and (3) a discussion of how the concept of network-centric warfare is related to the strategy of transformation as outlined in Joint Vision 2020 (JV 2020). At the time of this Congressional request, video teleconferencing, satellite communications, digital data and voice

communications systems, and GPS navigation and timing tools were already commonplace. The challenge DoD faced was how best to integrate NCW capabilities into a transforming military force. Many of the information technologies that DoD adopted to support military transformation were enabled by and heavily reliant upon space-based assets.

Current Environment

When one examines the power of the network in recent and ongoing military operations in Afghanistan and Iraq, it is quickly apparent that space is the critical enabler of intelligence, surveillance, and reconnaissance (ISR), and command and control (C2) communications capabilities. Joint Direct Attack Munitions (JDAM) from U.S. Air Force and U.S. Navy airframes rely upon GPS and Military Satellite Communications (MILSATCOM) for coordinating attacks on laser designated targets.[7] Unmanned Aerial Vehicles (UAVs) such as *Hunter, Predator,* and *Global Hawk* provide near real-time sensor-to-shooter links via satellite communications (SATCOM). The Force XXI Battle Command Brigade and Below/Blue Force Tracking (FBCB2/BFT) systems use GPS and space-based sensors to pinpoint and monitor units on the battlefield and provide unprecedented situational awareness to commanders. Each of the military services is integrating space-enabled information systems, sensors, relays, and IT to leverage the NCW capabilities of a networked joint force. The U.S. Air Force's *Air Force Command and Control Constellation* network integrates C2, ISR, tankers, space, ground, and sea-based systems.[8] The U.S. Navy and U.S. Marine Corps will invest heavily in IT to maximize shared battlespace awareness with *FORCENet*, a system critical to its Sea Power 21 Concept for Sea Basing.[9] The U.S. Army is already employing NCW-enabled systems in combat, and continues to develop NCW essential capabilities for the future that will comprise the *LandWarNet* –the Future Combat System (FCS), the Joint Tactical Radio System (JTRS), and Warfighter Information Network-Tactical (WIN-T). All these systems are networked across multiple frequency spectrums, are enabled by space, and carry a hefty price tag.

Clearly, a critical mass of the Joint Force must be robustly networked in order to enable NCW. Already, IT expenditures for this "critical mass" are staggering. The costs of building and expanding the GIG are in the tens of billions of dollars.[10] Each Global Hawk UAV system, which includes an aircraft, ground station and integrated sensor suite, has grown from an initial cost of $18 million to a current price of $48 million. If one factors recurring expenses, the price tag for each system approaches $70 million. The Predator UAV carries a $40 million per unit cost.[11] The Navy-Marine Corps Intranet (NMCI) alone carries a price tag of $6.9 billion.[12] DoD spending for communications and electronics systems that support NCW approached $60 billion

in 2006.[13] The power of NCW has not only captured the combined imaginations of the military and commercial industry, it has also captured their pocketbook.

Currently, no single nation-state can afford to match the total defense effort of the United States. Nonetheless, this economic reality does not preclude America's adversaries from competing.[14] They are obliged, through economic or technical necessity, to try and find cheaper, asymmetric methods of warfare, and exploit available weaknesses in what can be considered NCW's center of gravity—space-enabled IT systems. As spending for IT systems has skyrocketed and proliferation of space-enabled NCW technology has increased, so has the risk and vulnerability of this vast networked information infrastructure, specifically the space component. Space systems generally comprise three primary elements: a space element consisting of satellites, a terrestrial or ground-based element that includes supporting ground facilities for tracking, telemetry and control (TT&C), and a transmission link element that connects the space and ground elements via the electro-magnetic frequency spectrum. Adversaries will seek to disrupt or destroy U.S. space-based assets by attacking satellites, ground facilities, or communications networks, and seriously endanger U.S. warfighting capabilities.

Space Segment Vulnerabilities

Commercial/Leased SATCOM

In order to support the high bandwidth requirements of today's warfighter operating in a NCW environment, U.S. military forces have become increasingly dependent on commercial satellites. These commercial space assets provide the needed surge bandwidth capacity across the frequency spectrum to enable the high bandwidth requirements of NCW. A number of limitations, and hence vulnerabilities, present themselves when considering the DoD's reliance upon leased commercial space assets.

Assured availability of commercial space assets is a prime concern, especially in geographical areas with numerous, highly-populated metropolitan areas, because DoD must compete with commercial industry or other governmental agencies in order to secure satellite transponder leases. During the early stages of Operation Iraqi Freedom in 2003, the Defense Information Systems Agency (DISA) was severely challenged in securing Ku-Band satellite transponders for DoD, as it was in direct competition with U.S. and foreign news agencies, who also sought to obtain these valuable assets to cover the Iraqi invasion. Geographical areas that are completely void of large metropolitan concentrations are not financially rewarding to providers of leased satellite bandwidth, and therefore often times remain uncovered. Such was

the case for DISA in the fall of 2001 when it sought to lease surge bandwidth capacity in support of Operation Enduring Freedom. Few leased transponders were available that covered the sparsely-populated area of Afghanistan.

Leased transponder costs, while not an implicit vulnerability, are very much a fiscal limitation. In order to secure available commercial transponders for Operation Enduring Freedom, DISA had to execute two-year leases, even though it did not know at the time that those transponders would be required for the full duration. In some cases, leases are in-place in certain areas of the world, to ensure surge bandwidth will be available, should the DoD requirement arise. During the 2006 LandWarNet Conference, the U.S. Central Command (CENTCOM) Combined Forces Land Component Command (CFLCC) C-6, MG Dennis Lutz, explained that the annual cost for CENTCOM's leased transponders had risen from $74 million in 2001 to over $250 million in 2006. When considering surge bandwidth requirements across each Combatant Commander's Area of Responsibility (AOR), the costs become overwhelming as demand for services continue to rise.

Leased U.S. and foreign commercial satellites present additional vulnerabilities in terms of the necessary space hardening of satellite busses and payloads, as well as on-board systems redundancy. All satellites have a minimal level of hardening required to withstand the known hazards of the space environment, however, MILSATCOM and NATO satellites employ additional measures to mitigate the most extreme phenomena such as scintillation (natural or man-made), solar flares, and sporadic electromagnetic space radiation. Leasing mission essential warfighting capabilities from a U.S. commercial or foreign source risks foregoing these on-orbit protections. Moreover, few foreign commercial satellite providers employ redundant ground control capabilities (dual-diversity) in order to maintain continuity of space operations in the event of on-orbit disruption due to environmental conditions.

Space Situational Awareness Capability

Supporters of NCW assert that the main reason why no plan survives initial contact with the enemy is that situational awareness steadily deteriorates. It is reestablished periodically, only to degenerate again. By contrast, netting the joint forces will create high awareness and facilitate maintaining situational awareness, improving the ability to deter conflict, or prevail in conflict, should it become necessary.[15] Much the same can be said of the United States' space situational awareness capability. Once a robust defensive system to track and counter Soviet satellites during the Cold War, the DoD's ability to accurately track and monitor the position of other satellites in space relative to U.S. satellites, and developing systems that can neutralize or

destroy those viewed as a threat deteriorated when the Cold War ended and defense budgets declined during the 1990s.[16] As more nations become capable of launching commercial and military satellite communications and sensor payloads into space, and conducting space-based research to counter the NCW advantages employed by the U.S. military, there is a pressing need for the United States to know foreign satellites' capabilities and intentions in orbit. Lt. Gen. Michael Hamel, director of the Air Force's Space and Missile Systems Center, admits that the U.S. defense community has lost much expertise in monitoring and analysis capability, and that development of an Air Force Space-Based Surveillance program that will give the military a robust space monitoring capability is critical. Such a capability must employ both ground- and space-based systems to react to space-based threats and defend U.S. satellites from attack.[17]

China's robust microsatellite program is developing a counterspace capability that employs small, agile, and lightweight satellites as secondary payloads that are difficult to detect on otherwise overt space missions. Once on orbit, these *microsats* could then maneuver into position for attack. An effective space-based surveillance program could ensure maneuvering vehicles in space are detected in time to permit defensive action.[18] While space situational awareness and the ability to react defensively remains a challenge for the United States in the near term, there are alternative means, both passive and active, by which space-based assets may be protected, or their loss of services minimized. Robert Joseph, Undersecretary of State for Arms Control and International Security, in a December 2006 speech to the George C. Marshall Institute stated that "such alternatives include non-space (terrestrial) back-up systems, satellites with on-board subcomponent replacement parts and systems, satellite maneuvering systems to avoid threats, and other system security, data encryption, and communications frequency shifts."[19] While such alternative protective means provide a base level of risk mitigation for space assets, it is clearly not a viable substitute for an effective space situation awareness program.

Nation-State Attacks

Antisatellite (ASAT) systems are designed to exploit a number of susceptibilities of on-orbit space assets, and can generally be classified into two categories: directed energy weapons and interceptors. While the design of most MILSATCOM space assets have a significant level of hardening to account for space environmental effects and some known ASAT effects, few of the military's commercially leased satellites share this level of hardening and are thus susceptible not only to ASAT threats, but also a wide array of environmental conditions, including space anomalies, weather (solar activity), and scintillation. Because of the costs

involved in research and development of ASAT technologies, the required deployment of a network of space-tracking sensors, and the launch facilities required to effectively employ these systems, ASAT systems are generally within the purview of nation-states.

ASAT interceptors employ a number of concepts, but are essentially launched from a surface-, air-, or space-based platform directly toward its space-based target, or within a specified kill radius, in order to damage or destroy the satellite. Interceptors used as kinetic impact weapons cause satellite structural damage by impacting the target with warhead fragments, or the warhead itself. Chemical weapons can also be employed in interceptor warheads to surface-coat a target satellite with reacting chemicals designed to damage thermal control materials, solar panels, sensors, and antennas.[20] Low-altitude, direct ascent ASAT interceptors are launched on a booster from the ground or from an aircraft into a suborbital trajectory designed to intersect that of a Low Earth Orbit (LEO) satellite. High-altitude, short-duration interceptors are launched from large space launch vehicles into a temporary parking orbit, from which the interceptor maneuvers to engage Medium Earth Orbit (MEO), geosynchronous orbit, or Highly Elliptical Orbit (HEO) satellites, usually within 1-12 hours. Long-duration orbital interceptors are launched into a storage orbit, where they await the command to engage a target satellite. Plausible concepts for long-duration orbital interceptors include space mines, orbiting interceptors, and space-to-space missiles.[21]

Options also exist for ground-launched missiles, fragmentation rings, and high-altitude nuclear bursts that supercharge the Earth's Van Allen radiation belts, rendering non-hardened space assets ineffective or destroyed. These options offer the advantage of a hard-kill, but are non-discriminatory—enemy and friendly satellites alike would be damaged or destroyed by residual debris and radiation.[22] On January 12, 2007, China successfully employed a ground-based ASAT interceptor missile to destroy one of its own aging weather satellites orbiting at an altitude of roughly 530 miles. The test confirmed that China has the capability of hitting U.S. military ISR platforms at LEO altitudes that are used for intelligence, counterterrorism, and commercial purposes.[23] The debris from China's ASAT test is expected to orbit earth for at least 20 years and poses risk to some 800 LEO satellites, 400 of which are American.[24] Both Russia and China have an advanced array of operational and conceptual ASAT interceptors. It should be noted that despite Russia's call for a moratorium on the deployment of space weapons and recent declaration that it "shall not be the first to place any weapons in outer space," the former Soviet Union twice tested co-orbital *shotgun* type ASAT devices in space in 1977. Russia also continues to market various air-launched ASATs, and has been instrumental in the development of China's ASAT program.[25]

Directed-energy ASAT weapons tend to be more sophisticated, and also come in a variety of configurations. Ground-based high-powered lasers can damage thermal control, structural and solar power generation components on LEO satellites. Airborne high-powered lasers perform similar functions as ground-based lasers, but have the advantage of being mobile and operating above inclement weather that can limit ground-based laser effectiveness.[26] Space-based neutral particle beam weapons emit concentrated beams of neutral particles, typically hydrogen atoms, which can be propagated over long distances in outer space. Low-power antisensor lasers can blind or damage satellite-borne optical sensors. Low-power lasers are especially suitable for targeting space sensors, because the sensor amplifies the laser, which is operating in the same wavelength as the sensor. Moreover, antisensor laser ASATs can be employed against satellites operating at nearly any altitude. In September 2006, the Pentagon acknowledged that China had fired high-power ground-based lasers at a U.S. optical reconnaissance satellite flying over its territory in order to blind it, and prevent it from taking pictures as it passed overhead.[27] While it is unclear when China first used lasers to attack U.S. satellites, there have been several tests over the past few years, and the DoD remains quiet on the effectiveness of these disruptive attempts by China.

While the full extent of China's ASAT capabilities are not clear, U.S. experts agree that the People's Liberation Army (PLA) space program's goal is to obtain space-related information dominance coupled with the ability to disable its opponents' space assets in order to disrupt their space-based information and navigation systems in times of conflict.[28] Chinese military strategists write openly about exploiting the United States military's vulnerabilities created by heavy reliance on advanced space technology and an extensively networked C2 and ISR infrastructure it uses to conduct military operations. In his 2005 book, "Joint Space War Campaigns," Chinese PLA Colonel and author Yuan Zelu proposes covert deployment of ASAT weapons directed against U.S. space assets with "an orbiting network of strike weapons that will be concealed…and bring the opponent to his knees." [29] China's approach extends beyond destroying or disabling military space-based targets; it also includes targeting key commercial and financial systems that rely on satellite communications networks, thereby creating an effects-based approach to disabling an adversary's advanced technology advantage.[30]

Transmission Systems Vulnerabilities

Cyber Attacks

The cyber threat to DoD computer networks is real and poses a significant risk to the assured access and availability of critical warfighting systems that are networked into the GIG.

While there are malicious network intrusions, hacker attacks, and sabotage threats from within the United States, the great majority of computer network attacks emanate from the United States' peer military competitors: Russia and China. In 2005, China's PLA began embedding offensive computer network operations (CNO) into its military exercises, and has incorporated a first strike CNO strategy into its military doctrine, with the intent of achieving electromagnetic dominance in time of conflict. China openly practices military doctrine that combines CNO with electronic warfare, kinetic strikes against C2 and computer network nodes, and virus attacks on enemy battle command systems.[31] The PLA also employs its considerable civilian computer expertise from academies, institutes, and IT industries to support PLA operations by conducting hacker attacks, network intrusions, and other forms of cyber warfare.[32]

Because the DoD has more computers than any other U.S. department or agency—about 5 million worldwide—it's computers and the networks they traverse are very much exposed to foreign as well as domestic hackers. Consequently, the space control systems and the battlefield systems that are space-enabled are at risk and require hardening. In August 2005, the DoD revealed that it was experiencing nearly 500 attempted intrusions daily, from domestic sources and from the more than 20 nations that possess dedicated computer attack programs—mostly from China, North Korea, and Russia.[33] The majority of those attacks used web sites traced to the Chinese province of Guangdong, targeting U.S. military unclassified networks. The DoD revealed that during a 30-day period in July and August 2005, several large military computer networks, as well as networks of the departments of State, Energy, and Homeland Security were breached and in some cases disabled.[34] Similarly, in August and September 2006, cyber attacks on the computer systems of the Department of Commerce forced replacement of hundreds of computers, and lock down of Internet access for one month. A three-year U.S. investigation into the origins of such cyber attacks, code named *Titan Rain*, confirms that these computer network penetrations are increasingly coming from China.[35] Clearly, space-enabled NCW systems, whether C2, intelligence, space and missile warning, or even logistics, invite substantial risk where there is reliance on unclassified computer systems and where critical computer nodes are unprotected.

Commercial-Off-The-Shelf (COTS) Software/Computer Chips

The stark reality of today's IT economy is that much of the COTS software and many COTS electronic computer chips and other associated hardware are produced and coded in foreign markets. Not only is the U.S. becoming more dependent on foreign resources to meet its interests, but it also is becoming vulnerable to foreign-produced software and computer

devices that could contain malicious logic. The high dependence on COTS software increases the potential and impact of cyber attacks.

In recent years, software has been one of the first skill-intensive industries to move from the United States to the low-wage economies of developing countries. India, Ireland, Israel, China, and Brazil have postured themselves as emerging-market countries in the software industry, collectively accounting for more than $60 billion in exports in 2002. Software related activities generally fall into one of three categories: design, coding, or maintenance. While most of the functions that have been offshored (especially to India) involve coding and maintenance, product design for the time being, remains an in-house activity for most large U.S. software companies.[36] However, the vulnerability for software code written offshore, and computer chips produced in foreign countries that could be employed in critical space-based systems and ground-based computers networked into the GIG, bears close examination. While the DoD takes precautions to ensure its software design needs are met by U.S. companies, the same precautions are not always observed by U.S. defense contractors, their subcontractors or U.S. allies, and could leave the military open to damaging software attacks.

Electronic Warfare

Electronic attack against satellite transmission systems generally takes two forms: uplink jamming or downlink jamming. All military and commercial satellite communications systems are susceptible in varying degrees to both types of jamming. Uplink jamming targets a satellite's radio receiver component of the transponder, including sensors and command receivers, and it usually requires high-power transmitters.[37] If the satellite is geosynchronous, the receiver is generally used by customers covering a large area of the earth and the jamming can therefore have global effects. Numerous reports of uplink jamming and disruption of both communications and imaging satellites have surfaced recently.

During much of July 2003, two transponders of the commercial communications satellite Telstar 12, owned and operated by Loral, were intentionally jammed, disrupting digital television and radio broadcasts to Europe and the Middle East. Both transponders reportedly carried programming "likely to be offensive to the Iranian government," including Voice of America Persia, a broadcast service of the U.S. Government.[38]

Downlink jamming can affect communications links as well as satellite navigation signals, and requires much less power to be effective. The targets of downlink jamming are typically ground-based satellite receivers, ranging from large, fixed ground sites to portable, handheld GPS receivers. During the early phases of Operation Iraqi Freedom, Saddam Hussein's forces

employed Russian-made GPS jammers against coalition forces.[39] Although this attempt at disrupting coalition navigation and munitions targeting efforts ultimately failed, it speaks volumes to the means that our adversaries will employ in an attempt to neutralize U.S. space-based assets.

Ground Segment and Bandwidth Vulnerabilities

Ground Station Vulnerabilities

Ground segment attack or sabotage to disrupt space assets is an attractive option to low-technology or cash-strapped groups such as terrorists or transnational insurgents. Critical ground control facilities associated with U.S. space systems, both military and civilian, are targets to terrorist cells and foreign special operations forces. While military ground control facilities are located on DoD installations across the world to service the various satellite constellations, as well as provide redundancy for continuity of operations, they also have the added benefit of being operated and secured by military personnel. Commercial ground control facilities in the U.S. and overseas generally don't have that luxury. Adversaries need only to glean information about which ground facilities are critical to the U.S.—especially those that offer non-redundant vulnerabilities—and where they are located. Unfortunately, many of these facilities are described in open-source reference materials.

Foreign commercial satellite providers present additional vulnerabilities in terms of their satellite ground control facilities and ground control redundancy. Leasing critical warfighting capabilities from a foreign source presents its own risks. Beside the risk of assured access and availability for U.S. forces, the DoD can not oversee what potential adversaries may have access to foreign commercial ground control facilities, nor are these facilities necessarily accorded the same level of physical security as U.S. satellite ground control facilities. Such vulnerabilities at these facilities render them susceptible to unauthorized monitoring or even sabotage of U.S. leased assets. Another inherent risk of using any advanced technology is that failures will occur, and when these failures occur at commercial or foreign ground control facilities, redundant paths for communications circuits and sufficient on-hand bench stock (e.g. spare parts) that maintain continuity of operations are paramount. If the communications architecture is not engineered to be sufficiently robust, allowing both equipment and path redundancy, then the U.S. increases its vulnerability to enemy actions. Not all foreign commercial satellite providers employ a sufficiently redundant ground control capability for continuity or reconstitution in the event of ground system or power failures.

Bandwidth

Though often acknowledged as a limitation but not a vulnerability, electro-magnetic frequency spectrum, or bandwidth, is a finite resource, and is in fact a limitation *and* a vulnerability. In the 1990s, the U.S. military lacked sufficient bandwidth, but did not need to share information outside the force. Now, it has much more bandwidth, but it also has to share data across the joint force and interagency domains as well as satisfy multinational requirements in order to enable NCW. The DoD employs communications and intelligence systems and weapons platforms with large imbedded bandwidth requirements at nearly every segment of the electro-magnetic frequency spectrum. From the Extremely Low Frequency (ELF) requirements of submarines at sea to the Extremely High Frequency (EHF) requirements of the nuclear-capable global strike force, the DoD's ability to provide the warfighter with assured bandwidth to enable NCW capabilities continues to be challenged by the proliferation of emerging IT systems.

During Operations Desert Shield and Desert Storm in 1990-91, the DoD experienced a marked increase in the satellite communications bandwidth requirement for the CENTCOM AOR. A large Army and Marine ground force, the introduction of systems such as the Air Force's Joint Surveillance and Target Attack Radar System (JSTARS), and precision guided munitions combined to place a 48 MHz bandwidth requirement on CENTCOM that could not be satisfied by MILSATCOM assets alone. The DoD was forced to physically reposition space-based military X-Band assets and execute commercial satellite transponder leases. By June 2003, the combined CENTCOM bandwidth requirements for Operations Enduring Freedom and Iraqi Freedom had ballooned to 2.8 GHz and by November 2005 the CENTCOM AOR bandwidth requirement was in excess of 3.5 GHz, supported by nine satellites.[40] The Army's Center for Lessons Learned recently released its report on V Corps in the drive to Baghdad, "On Point: The U.S. Army in Operation Iraqi Freedom." The report details the lack of bandwidth accorded to the Army's intelligence teams that had to share a 1 Mbps satellite connection with up to 20 separate command posts to deliver 256 kbps imagery files. Imagery was rarely delivered on time, and basic voice communications among the command posts suffered constant interference.[41]

The Army's Future Combat System (FCS) program relies on IT systems integrated among its 18 separate platforms, ranging from robotic ground and air systems to a family of lightweight mulitimission manned vehicles. All of these platforms will be linked to the FCS computer network, sharing tactical data across the battlefield. Each of these platforms has a substantial bandwidth requirement that is enabled by space-based sensors and communications

satellites.[42] The Army acknowledges that the key to the entire FCS program is a space-enabled network consisting of a system-of-systems common operating environment (SOSCOE), battle command software and intelligence, surveillance and reconnaissance systems. As these 18 separate FCS platforms operate in relative close proximity with other U.S. and coalition air and sea communications, weapons, and intelligent munitions systems, it becomes clear that the FCS bandwidth requirements become a limitation to U.S. forces, and the FCS space-enabled integrated network becomes a vulnerability that an adversary will seek to exploit. Moreover, competing requirements among joint battlefield systems for bandwidth within limited frequency bands can cause radio frequency interference and significantly reduce the effectiveness of all joint battle command and combat platforms across the battlespace.

At the 2006 LandWarNet Conference, the Joint Staff J-6, VADM Nancy Brown cited bandwidth and frequency interference problems that continue to emerge in ongoing operations in Iraq and Afghanistan. VADM Brown related one bandwidth conflict in a convoy in Iraq in which an electronic countermeasures system for defeating improvised explosives devices (IEDs) conflicted with a radio used for calling for fire support and rapid reaction forces. Both systems nullified one another, so the convoy lost both capabilities.[43] In a NCW environment, bandwidth can indeed be both a limitation and a vulnerability.

Proceed With Caution

Conclusions

The United States' leveraging of space technology has created demonstrable asymmetric advantages as well as strategic vulnerabilities for the military and commercial industry. The DoD's NCW vision is a natural consequence of advances in IT, its principle enabler is space, and it is here to stay. Space capabilities are integral to networking modern warfighting forces, and are recognized force multipliers that increase combat effectiveness by providing critical ISR, weather, navigation, timing, missile warning, C2 and communications capabilities. As British author Colin S. Gray remarked when extrapolating Clausewitz's ideas for the future of space-enabled warfare:

> Countries have 'centres of gravity' key to their functioning. A country's or coalition's ability to wage war successfully can be negated if those centres of gravity are menaced, damaged, or taken.[44]

The DoD's reliance on space makes its space-based assets the center of gravity for warfighting effectiveness and the primary target for adversaries, and requires that the weaknesses and

potential vulnerabilities of NCW be identified and addressed in order to deny the enemy any unchallenged success.

America's dominance of spaced-based intelligence, navigation, sensors, relays, and other satellite capabilities is rapidly changing. The proliferation of space technologies across the world and increased availability of inexpensive space countermeasures threaten the space assets on which the U.S. military relies to execute battle command and ensure battlespace supremacy in the 21st century. Adversaries recognize the benefits conferred by space systems on nations that rely on them, and will exploit space vulnerabilities using a wide array of counterspace techniques, including passive means such as denial and deception, and more active means such as ground segment attack, sabotage, and cyber attack to degrade US space capabilities. Clearly, the disruption, denial, degradation, or destruction of space systems and space-enabled services could seriously affect U.S. warfighting capabilities, and there are sufficient recent experiences that justify immediate enactment of measures to defend against and mitigate these vulnerabilities.

Recommendations

A crucial first step in undertaking any space vulnerability countermeasures is a valid assessment of current capabilities (friendly and enemy) coupled with a sound definition of core organizational competencies across the DoD. Not all military service components share the same vulnerabilities or the resources and capability to mitigate threats. The Office of the Secretary of Defense, Networks and Information Integration (OSD/NII) would be a starting point for consolidating and integrating service-specific vulnerabilities, and providing joint solutions that benefit the entire force. Services are often handicapped in correctly assessing threats and effectively employing countermeasures because of their core identity or mission that has been reinforced over time. OSD/NII could provide leadership in consolidating and identifying space technology vulnerabilities and making the security of our national space-based assets a priority for resourcing and a core competency across the services. Moreover, OSD/NII must prepare the solutions for allied interoperability, as U.S. advances in IT threaten to isolate potential coalition partners' ability to coexist with the U.S. military on the battlefield.[45]

The joint community, and especially the Army, must embrace electronic warfare (EW) as an enduring core competency in order to use electromagnetic energy for attack, defense, and sensing capabilities that are fully integrated and synchronized with joint operations. Military occupational specialties must be developed for enlisted and commissioned officers to combat the threat and ensure access to the electromagnetic spectrum. Employing passive and active

means of electronic warfare is a recognized form of effects-based (non-kinetic) fires that can add an important dimension to the battlefield and save lives while denying enemy control of the electromagnetic spectrum.

Reliable access to space assets is a key consideration for military applications, and requires ground control path *and* systems redundancy. The development of mobile, survivable satellite ground segment infrastructure for all critical frequency bands, not just nuclear C2 nets, is prudent and justified. Satellite telemetry, TT&C functions, traditionally accomplished using large, fixed stations, can be performed by small, transportable equipment. Mobile TT&C stations, although currently not in widespread use, should be a U.S. consideration that can provide greatly enhanced flexibility to a critical aspect of satellite systems operations.[46]

When analyzing China's published military strategy and its aggressive counterspace programs, it is clear that China intends to hold the U.S. military's critical space systems at risk. If the United States wants assured access to space-enabled communications, ISR, navigation, weather, missile warning, and munitions targeting, it must aggressively develop a space situation awareness program aimed at not only cataloging space objects between LEO and geosynchronous orbits, but also improving its ability to identify the origin and nature of attacks on its space assets, with the ability to instantly determine whether an attack was due to natural environmental factors or anomalies, such as radiation, or an attack by a hostile satellite or ground-based counterspace system.[47] The United States is better postured to deter aggression against its on-orbit assets if it possesses the ability to recognize indications and warnings of emerging threats, and have the ability to respond defensively or offensively when attacked.[48]

Finally, to the degree that the need for increased bandwidth is not fully satisfied, combatant commanders will be forced to make hard choices and trade off various systems when employing future combat forces. High-bandwidth systems such as Telemedicine and service support systems for logistics and transportation could become candidates to be off-loaded from MILSATCOM and leased commercial transponders onto terrestrial and undersea fiber in order to free critical bandwidth for the warfighter. While terrestrial telecommunications capabilities are expensive and not always available in remote areas of the world, their maximized employment and use is critical in freeing the available spaced-based frequency spectrum for the warfighter.

The vulnerabilities of employing space technology to enable NCW are known, will continue to be exploited by America's adversaries, and require a concerted, long-term effort to address the emerging threats. U.S. reliance on NCW in general, and spaced-enabled IT in particular, should not be in toto. Since space systems and electromagnetic spectrum availability

can not be guaranteed, especially during conflict, it stands to reason that the U.S. military must examine back-up methods and redundant systems to execute effective battle command. If NCW is to remain an enduring core competency of U.S. military warfighting capability, then let us take the appropriate countermeasures required to ensure that our space-based assets are protected and that our IT networks are secured from the strategic paradox that it is today.

Endnotes

[1] Susan Lawrence, "CENTCOM Pursues Assured, Interoperable Communications," *SIGNAL* (October 2006): 29-33.

[2] Tim Gibson, "What You Should Know About Attacking Computer Networks," *U.S. Naval Institute Proceedings* (January 2003): 48-51.

[3] Arthur K. Cebrowski and John J. Garstka, "Network-Centric Warfare: Its Origin and Future," *U.S. Naval Institute Proceedings,* (January 1998): 28-35.

[4] Ibid., 29.

[5] Nicolas G. Carr, *Does IT Matter?,* (Boston: Harvard Business School Press, 2004), 24.

[6] Richard B. Myers, "Understanding Transformation," *U.S. Naval Institute Proceedings,* (February 2003): 39-40.

[7] John Garstka, *Defense Transformation and Network Centric Warfare,* 2 September 2002; available from http://www.navyleague.org/membership/ncw.pdf; Internet; accessed 12 December 2006.

[8] Jeffrey L. Groh, "Network-Centric Warfare: Just About Technology?," in *U.S. Army War College Guide to National Security Policy and Strategy, 2nd Edition*, (Carlisle Barracks: June 2006): 380.

[9] Geoff Fein, "Info Sharing Will Be Vital in Future Combat Operations, Hagee Says," *Defense Daily,* 31 March 2005, p. 1.

[10] David W. Roberts and Joseph A. Smith, "Realizing the Promise of Network-Centric Warfare," White Paper (Norfolk: Joint Forces Staff College, 10 March 2003), 4.

[11] Leona C. Bull, "Air Force Wants Northrop to Cut Global Hawk Costs," *Journal of Aerospace and Defense Industry News* (17 May 2002): 1.

[12] Ernest Fagan, "Wired for the Future – The Navy Marine Corps Intranet," March/April 2001; available from http://www.navsup.navy.mil/lintest/marapr01/fagan.htm; Internet; accessed 27 December 2006.

[13] John Keller, "DoD Electronics Spending May Approach $60 Billion in 2006," *Military & Aerospace Technology* (14 April 2005): 3.

[14] Colin S. Gray, “Technology As a Dynamic Defence Transformation,” *Defence Studies* (March 2006): 37.

[15] Arthur K. Cebrowski and John J. Garstka, “Network-Centric Warfare: Its Origin and Future,” *U.S. Naval Institute* Proceedings (January 1998): 33.

[16] Greg Grant, “Air Force Seeks to Strengthen Satellite Defense System,” 1 November 2006; available from http://www.govexec.com/dailyfed/1106/110106g1.htm; Internet; accessed 27 December 2006.

[17] Ibid.

[18] Richard J. Adams and Martin E. France, “The Chinese Threat to US Space Superiority,” *High Frontier* (Winter 2005): 21-22.

[19] Bill Gertz, “U.S. to Defend Space with Military Force,” *The Washington Times,* 14 December 2006; available from http://ebird.afis.mil/ebfiles/e20061214473744.html; Internet; accessed 12 January 2007.

[20] National Air and Space Intelligence Center, *Challenges to US Space Superiority* (Wright-Patterson Air Force Base, March 2005), 21.

[21] Ibid., 22.

[22] Adams and France, 20.

[23] William J. Broad and David E. Sanger, “Flexing Muscle, China Destroys Satellite In Test,” *New York Times*, 19 January 2007, sec. A, p. 1.

[24] Bill Gertz, “Officials Fear War in Space by China,” *The Washington Times*, 24 January 2007; available from http://www.washtimes.com/functions/print.php?StoryID=20070124-121536-8225r; Internet; accessed 25 January 2007.

[25] Claude Lafleur, *The Spacecraft Enclyclopedia*, (Science-Presse, Paris, 2005), 12.

[26] Challenges to US Space Superiority, 24.

[27] Vago Muradian, “China Tried To Blind U.S. Sats With Laser,” *DefenseNews* (25 September 2006): 1, 6.

[28] U.S. Economic and Security Review Commission, *2006 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, D.C.: U.S. Government Printing Office, November 2006), 137.

[29] Bill Gertz, “Officials Fear War in Space by China,” *The Washington Times*, 24 January 2007; available from http://www.washtimes.com/functions/print.php?StoryID=20070124-121536-8225r; Internet; accessed 25 January 2007.

[30] Ibid.

[31] Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2006* (Washington, D.C.: U.S. Government Printing Office, March 2006), 31.

[32] Ibid., 35.

[33] Bradley Graham, "Hackers Attack Via Chinese Web Sites," *The Washington Post*, 25 August 2005, sec. A. p. 1.

[34] Ibid.

[35] 2006 Report to Congress of the U.S.-China Economic and Security Review Commission, 137.

[36] Ashish Arora, "The Emerging Offshore Software Industries and the United States Economy," *Brookings Trade Forum 2005*: 1-2.

[37] Robert K. Ackerman, "Space Vulnerabilities Threaten U.S. Edge in Battle," *SIGNAL* (June 2005): 1-6.

[38] Challenges to US Space Superiority, 20.

[39] Ibid., 4.

[40] Ron Dixon, "USCENTCOM Commercial SATCOM," briefing slides with scripted commentary, HQ, CENTCOM, 15 November 2005.

[41] Gopal Ratnam, "Bandwidth Battle," *DefenseNews* (9 October 2006): 37.

[42] Henry S. Kenyon, "Future Combat Systems Progress Remains Uncertain," *Signal* (November 2006): 47.

[43] Robert K. Ackerman, "Warfighters Fight the New Fight," *SIGNAL* (October 2006): 74.

[44] Colin S. Gray, *Modern Strategy* (Oxford University Press, New York 1999): 257.

[45] Groh, 381.

[46] Challenges to US Space Superiority, 15.

[47] Adams and France, 22.

[48] Ibid.